УДК 342:343.346.8
СОКУРЕНКО Валерій Васильович,
доктор юридичних наук, професор,
член-кореспондент Національної академії правових наук України,
заслужений юрист України,
ректор Харківського національного університету внутрішніх справ
https://orcid.org/0000-0001-8923-5639

ПРАКТИЧНА СКЛАДОВА ФАХОВОЇ ПРОФЕСІЙНОЇ ПІДГОТОВКИ КАДРІВ ДЛЯ ПІДРОЗДІЛІВ КІБЕРПОЛІЦІЇ НАЦІОНАЛЬНОЇ ПОЛІЦІЇ УКРАЇНИ

На сьогодні незмінною залишається тенденція останніх років у напрямі збільшення кількості та масштабності правопорушень у кіберсфері. За даними експертів, щорічні збитки від кіберзлочинів також стрімко зростають. Так, дослідники американської компанії McAfee, яка спеціалізується на комп'ютерній безпеці, та Центру стратегічних і міжнародних досліджень (CSIS) установили, що у 2020 році хакери завдали світовій економіці збитки у розмірі понад трильйон доларів, або 820 мільярдів євро, що становить понад один відсоток світового ВВП. Завдані цьогоріч хакерами збитки є на 50 відсотків вищими, ніж у 2018 році.

Ураховуючи той факт, що цифровізація світового суспільства також швидко набирає обертів, у найближчому майбутньому не слід очікувати стабілізації або зменшення темпів росту кіберзлочинності. Із цього випливає актуальність застосування всіх можливих факторів підвищення якості підготовки майбутніх кіберполіцейських.

Найважливішим чинником підготовки кіберполіцейських є практична складова навчання. Компонентами цієї складової у їх підготовці є такі: а) фахова практична спрямованість навчальних практичних і лабораторних занять, яка полягає у вирішенні практичних завдань професійної діяльності кіберполіцейських; б) рішення фахових завдань практичного спрямування в процесі написання курсових робіт, а також випускної кваліфікаційної роботи; в) отримання професійних практичних навичок під час навчальної практики.

Крім перелічених обов'язкових компонентів, які передбачено навчальними планами підготовки, важливу роль відіграють інші, нерегламентовані форми неформального залучення курсантів та викладачів до співробітництва з практичними органами у сфері протидії кіберзлочинності. У ХНУВС були запроваджені й результативно застосовуються такі форми залучення курсантів та викладачів:

– моніторинг кіберпростору з метою сприяння діяльності Департаменту кіберполіції та Департаменту кримінального аналізу НПУ в межах функціонування Центру боротьби з кіберзлочинністю та моніторингу кіберпростору ХНУВС;

– відпрацювання практичних навичок виявлення кібератак і реагування на них на тренінгових платформах Центру боротьби з кіберзлочинністю та моніторингу кіберпростору ХНУВС;

– співробітництво з громадською спілкою «Глобальний центр взаємодії кіберпростору» з метою сприяння вирішенню завдань з профілактики і запобігання онлайн-шахрайству, встановлення осіб кіберзлочинців та їх місцезнаходження;

– участь у проведенні тренінгів під егідою КМЕС та ОБСЄ для фахівців у сфері кібербезпеки та протидії торгівлі людьми як т'юторів;

– участь курсантів і викладачів у міжнародних тренінгових онлайн-платформах для фахівців у сфері кібербезпеки.

До особливостей застосування перелічених вище форм практичної підготовки можна віднести такі.

1. Високі вимоги до параметрів технічного забезпечення використовуваної комп'ютерної і комунікаційної техніки і, відповідно, її висока вартість.

2. Обмежені функціональні можливості безкоштовних тренінгових платформ і висока вартість розвинутих багатофункціональних тренінгових платформ.

3. Необхідність урахування вітчизняних і особливо міжнародних нормативних актів у галузі захисту персональної інформації під час моніторингу кіберпростору (здійснення заходів OSINT) для запобігання їх порушенням.

4. Відсутність (наразі) можливості практичного знайомства із сучасними платформами автоматичного моніторингу кіберпростору в режимі 24/7 для виявлення і прогнозування злочинної активності на основі «слабких сигналів».

Одержано 07.04.2021